



AFRICAHACKON

The background is a dark blue gradient. It features several abstract geometric elements: a large white arc on the left side, a smaller blue arc below it, and a yellow circle with a blue center at the bottom left. In the top right, there are blue and yellow lines forming a step-like pattern. On the right side, there are five horizontal yellow lines of varying lengths. At the bottom, there are blue and white lines forming a grid-like pattern. The title text is centered in a bold, yellow, sans-serif font.

Anti-malware Evasion in Corporate Networks and Defense Mechanisms



WHOAMI

- Security enthusiast
- E-kraal Innovation hub
- Research and Development
- Trainer
- Mentor

Contact:

- Twitter: @Nyawira1
- LinkedIn: marthanyawira
- Blog: t4tul4.github.io
- Email: nyawi@tutanota.com

AGENDA

01

INTRODUCTION

02

APC INJECTION

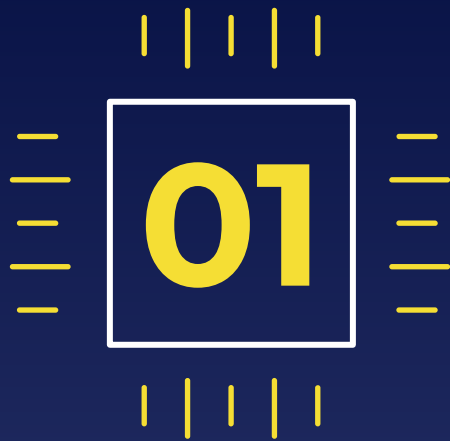
03

AMSI BYPASS

04

Defense
Mechanisms





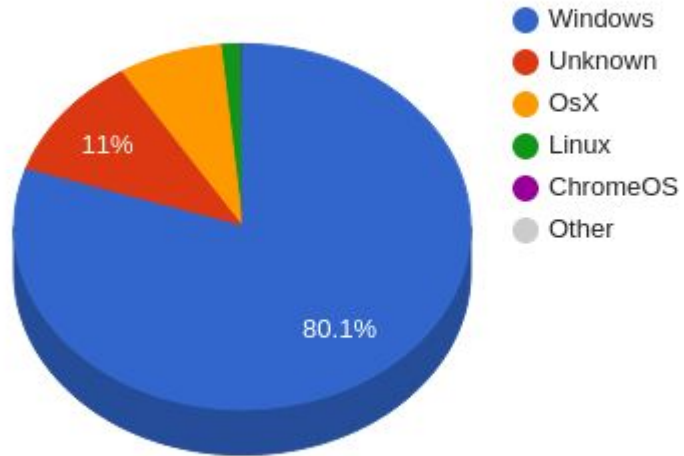
INTRODUCTION



STATISTICS



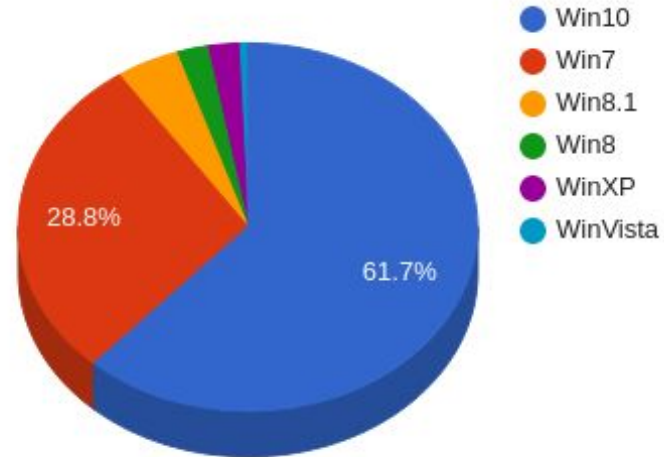
Desktop OS Market Share in Africa from Sept 2020 - Oct 2021



STATISTICS

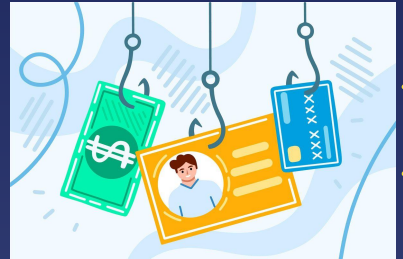


Windows Version Market Share in Africa from Sept 2020 - Oct 2021



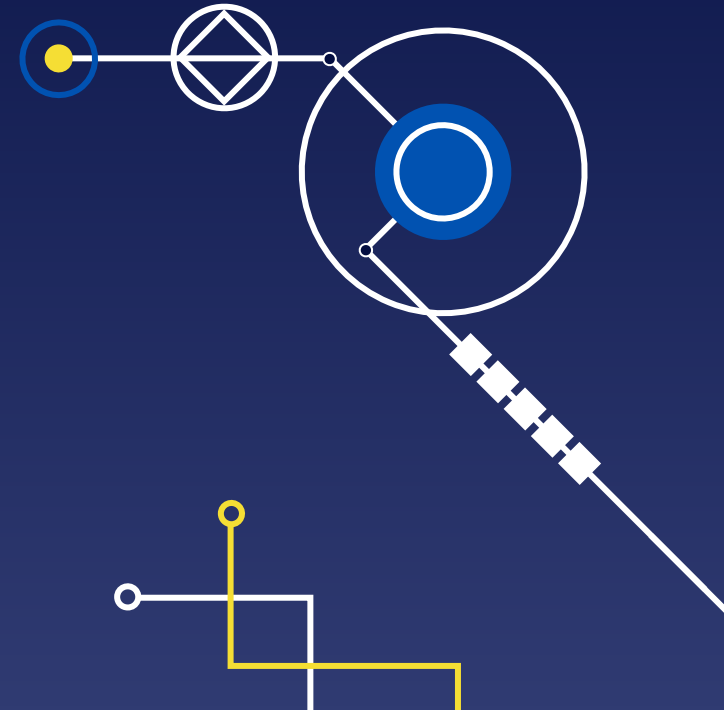
ANTI-MALWARE

- Anti-malware software looks for, detects, and eliminates viruses as well as other harmful software such as worms, trojans, adware, and others.
- Malware may cause a wide range of harmful behavior.
- They have the ability to
 1. Harvest data
 2. Restrict access to your files
 3. Disrupt Daily Operations
 4. Spread Throughout Your Network



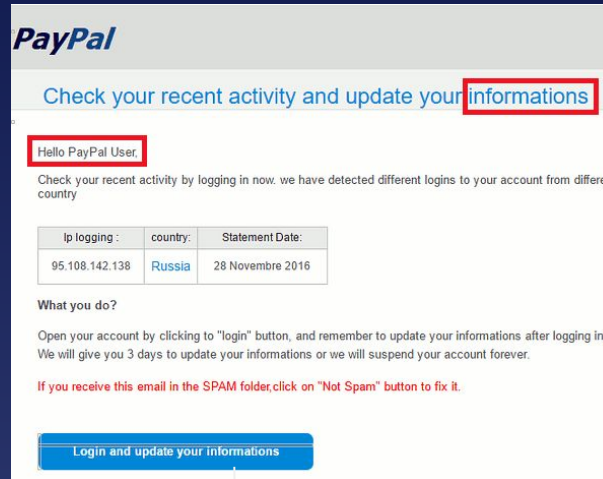
ANTI-MALWARE TYPES

- There are major three methods based on which Anti-malware are designed.



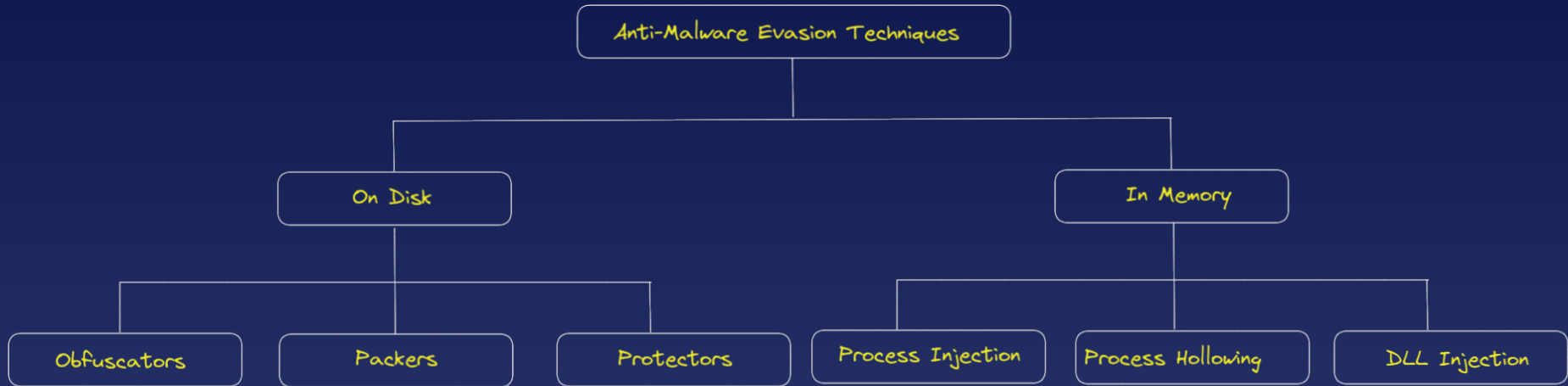
PHISHING

- Phishing is a type of social engineering attack often used to steal user data.
- The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware



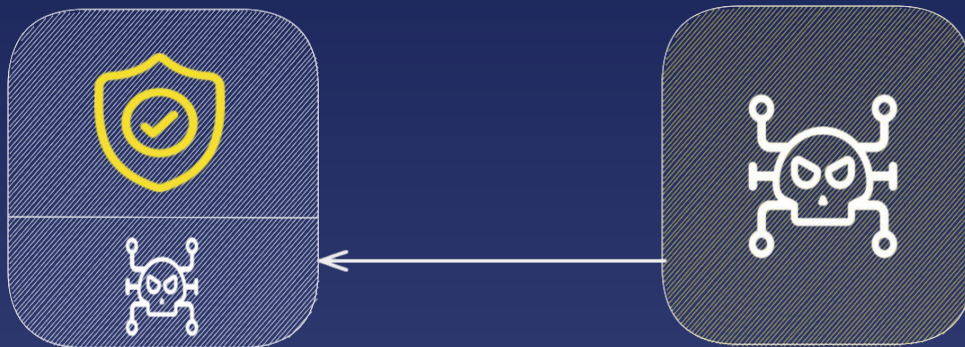
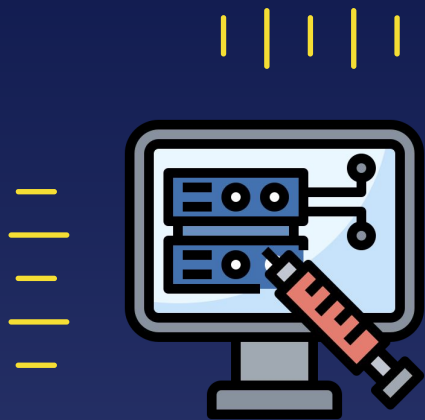
ANTI-MALWARE EVASION TECHNIQUES

- Anti-malware evasion is done by applying certain changes in code residing on disk or in memory.



Process Memory Injection

- It is a widespread defense evasion technique employed often within malware and entails running custom code within the address space of another process.
- They are numerous techniques but I will focus on Asynchronous Procedure Calls (APC) injection.



The background is a dark blue gradient. In the corners, there are stylized circuit board traces. Top-left: white and yellow lines with circular endpoints. Top-right: white lines with circular endpoints. Bottom-left: white lines with circular endpoints. Bottom-right: white and blue lines with circular endpoints. In the center, there is a white square containing the yellow text '02'. This square is surrounded by yellow horizontal and vertical lines, resembling a microchip's pins.

02

APC INJECTION

A horizontal blue line with small circular endpoints at each end, positioned directly below the title.

Flow Chart



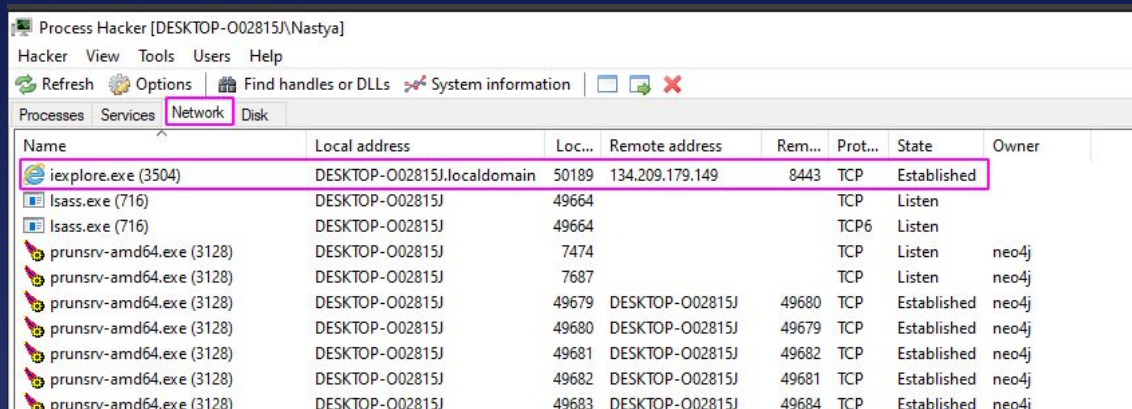
Generate a Covenant payload

- C2 server is a computer controlled by an attacker which is used to send commands to systems compromised by malware and receive stolen data from a target network.



Process Hacker

- A free, powerful, multi-purpose tool that helps you monitor system resources, debug software and detect malware.



Flow Chart



Generate a
Covenant payload



Obfuscate



Generate
Shellcode



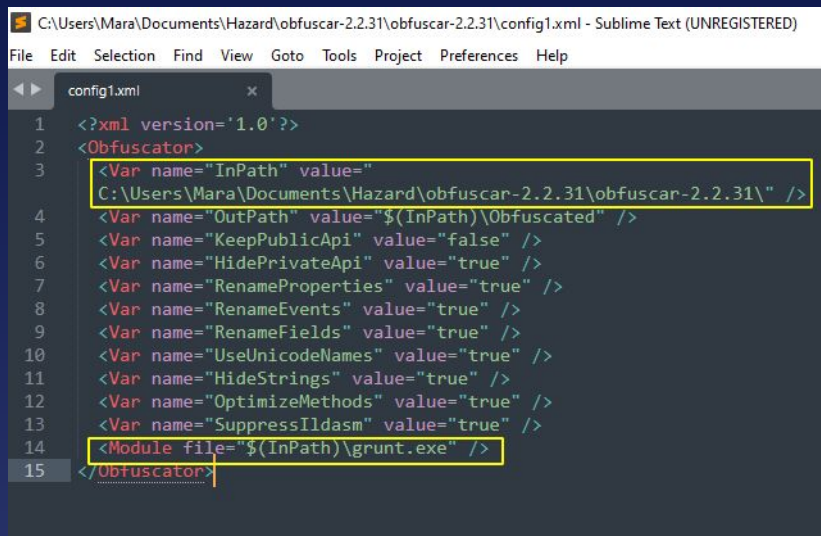
APC Injection



Generate a Fake
Certificate

Obfuscator

- Obfuscator is a basic obfuscator for .NET assemblies.
- An open source project backed by LeXtudio.
- It uses massive overloading to rename metadata in .NET assemblies to a minimal set, distinguishable in most cases only by signature.



```
C:\Users\Mara\Documents\Hazard\obfuscator-2.2.31\obfuscator-2.2.31\config1.xml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

config1.xml
1 <?xml version='1.0'?>
2 <Obfuscator>
3   <Var name="InPath" value="
   C:\Users\Mara\Documents\Hazard\obfuscator-2.2.31\obfuscator-2.2.31\" />
4   <Var name="OutPath" value="$(InPath)\Obfuscated" />
5   <Var name="KeepPublicApi" value="false" />
6   <Var name="HidePrivateApi" value="true" />
7   <Var name="RenameProperties" value="true" />
8   <Var name="RenameEvents" value="true" />
9   <Var name="RenameFields" value="true" />
10  <Var name="UseUnicodeNames" value="true" />
11  <Var name="HideStrings" value="true" />
12  <Var name="OptimizeMethods" value="true" />
13  <Var name="SuppressIldasm" value="true" />
14  <Module file="$(InPath)\grunt.exe" />
15 </Obfuscator>
```

Flow Chart



Generate a Covenant
payload



Obfuscate



Generate
Shellcode



APC Injection



Generate a Fake
Certificate

Donut



- Donut is a position-independent code that enables in-memory execution of VBScript, JScript, EXE, DLL files and dotNET assemblies.
- This tool was written by The Wover @TheRealWover
- After the file is loaded and executed in memory, the original reference is erased to deter memory scanners.

Flow Chart



APC INJECTION

- An asynchronous procedure call (APC) is a function that executes asynchronously in the context of a particular thread.
- Code by 3xpl01tc0d3r



Flow Chart



Install a C2 and
generate a
Payload



Obfuscate



Generate
Shellcode



APC Injection



Generate a Fake
Certificate

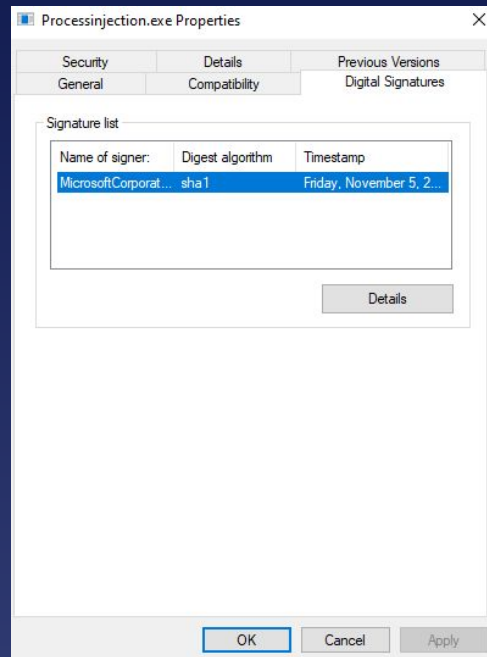
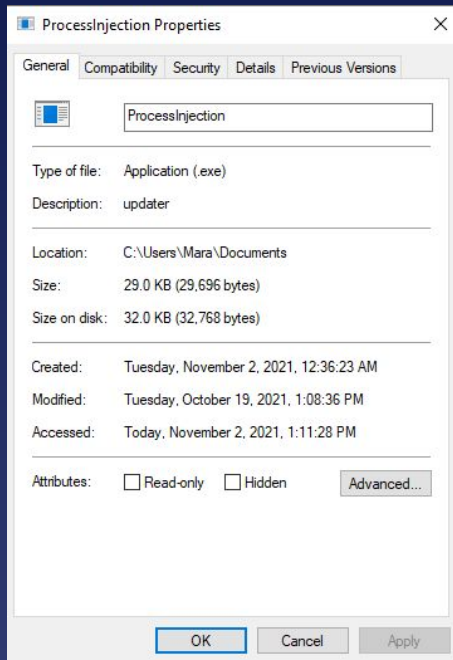
Forging Certificates

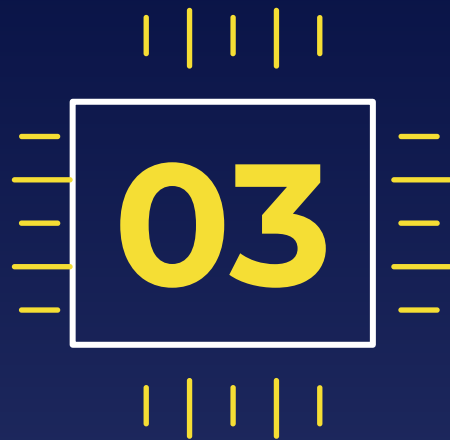


- Forging certificates involves the creation of fake or fraudulent certificate.
- Some anti-malware solutions check if an executable has a certificate if not the antivirus is triggered.

Lazy Sign

- Create fake certs for binaries using windows binaries and the power of bat files.
- Tool written by Jean jfmaes





AMSI BYPASS




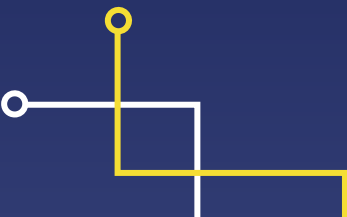

AMSI



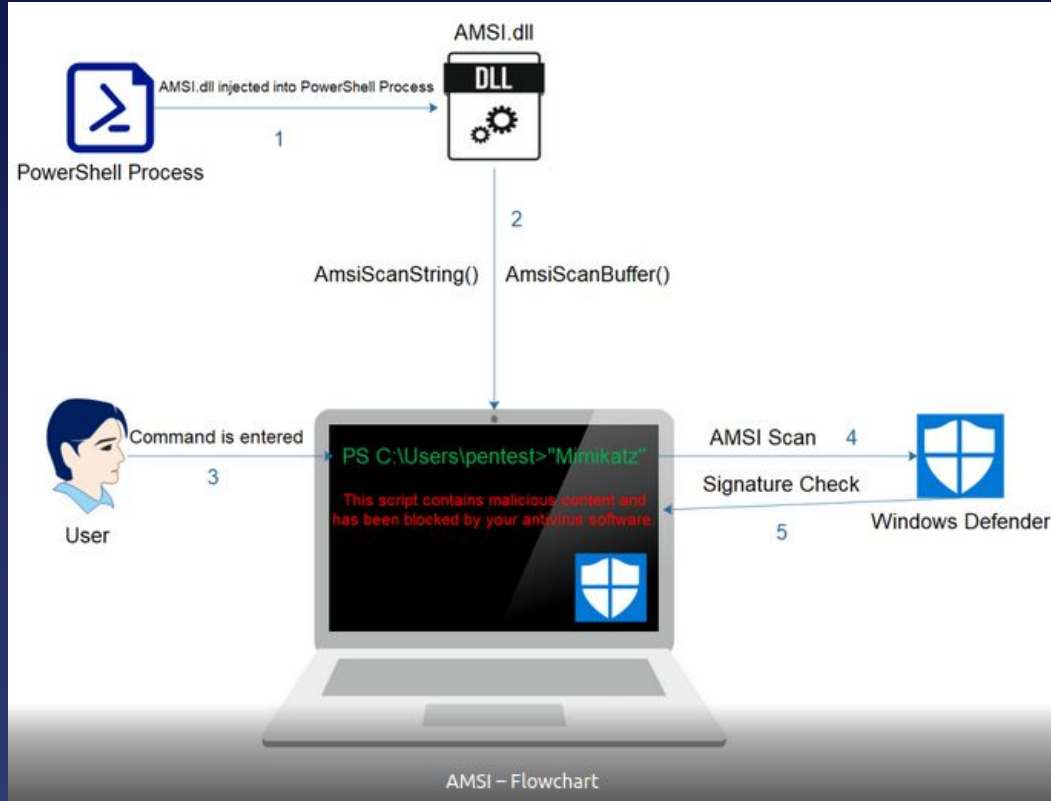
- The Antimalware Scan Interface is a set of Windows APIs that allows any application to integrate with an antivirus product.
- Windows Defender, naturally, acts as an AMSI provider as do many third-party AV solutions.



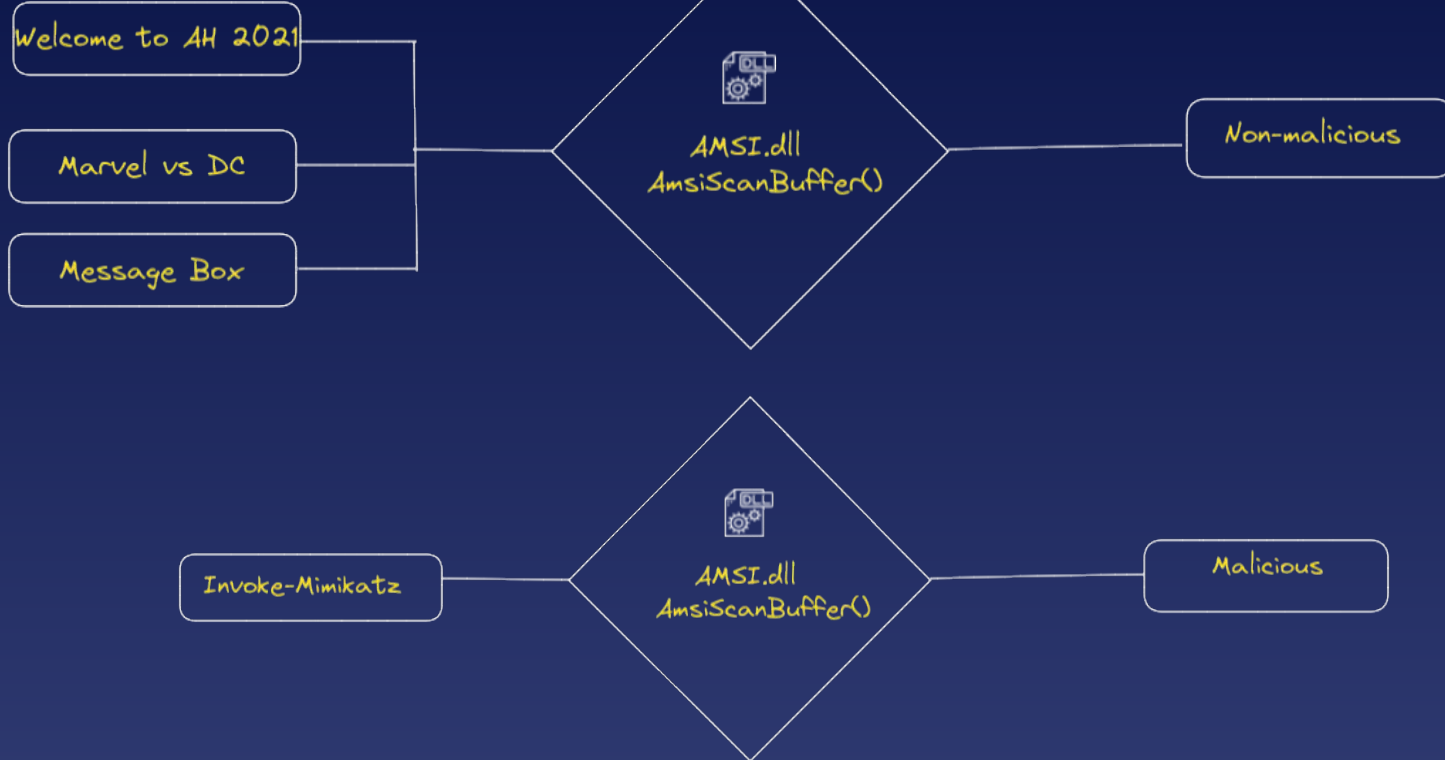
AMSI Windows Integration

- The AMSI feature is integrated into these components of Windows 10.
 1. User Account Control, or UAC (elevation of EXE, COM, MSI, or ActiveX installation)
 2. PowerShell (scripts, interactive use, and dynamic code evaluation)
 3. Windows Script Host (wscript.exe and cscript.exe)
 4. JavaScript and VBScript.
 5. Office VBA macros
- 
- 
- 

How AMSI Works

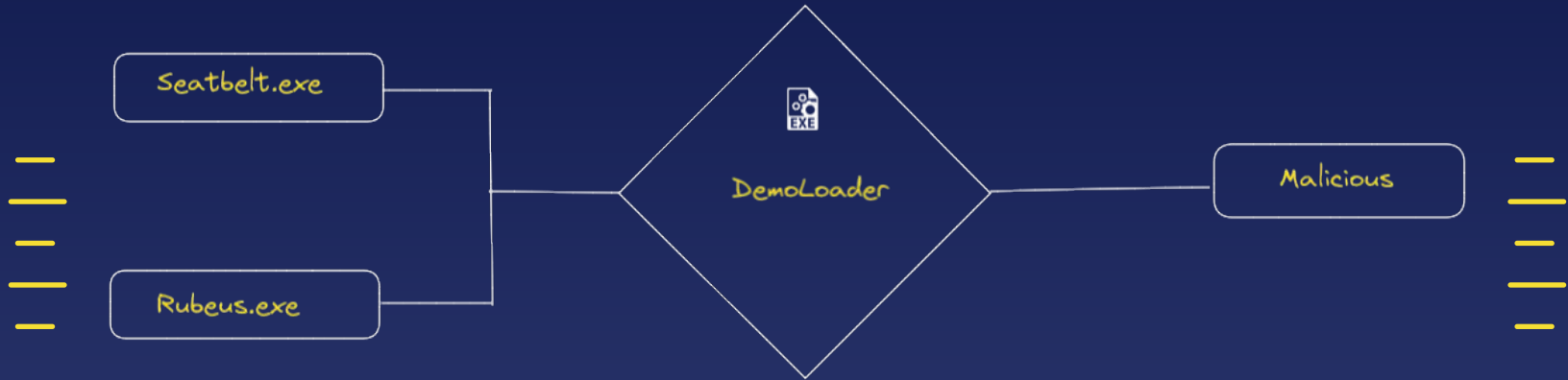


How AMSI Works



How DemoLoader Works

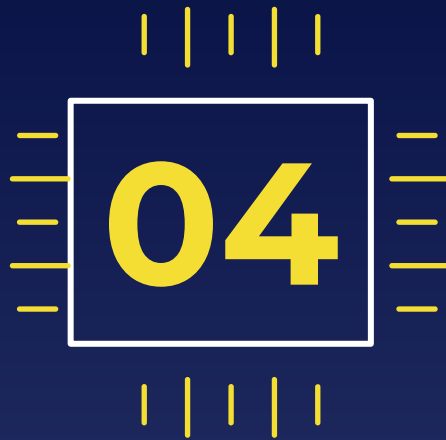
- DemoLoader is an executable that Downloads and executes .NET executables in memory



How DemoLoader_Patched Works

- DemoLoader is an executable that downloads and executes .NET executables in memory.
- It includes an amsiBypass patch.





Defense Mechanisms



Countermeasures

- Big organization that has huge amount of network devices and servers to manage must use Security Information and event Management (SIEM) systems like NetIQ, ArcSight or NetForensic etc.
- Incorporate pentesting into your cyber security posture as an organisation.
- Conduct end-users training to make them aware of various risks related to virus or worms attacks.
- The desktop Antivirus (AV) signature must be kept up-to-date.



Resources

[https://en.wikipedia.org/wiki/Evasion \(network security\)](https://en.wikipedia.org/wiki/Evasion_(network_security))

<https://www.nopsec.com/blog/pen-testing-toolkit-tools-techniques-used-to-evade-antivirus-software/>

<https://0xhop.github.io/evasion/2021/04/19/evasion-pt1/>

http://www.infosecwriters.com/Papers/DMohanty_AV_Evasion.pdf

<https://www.hivepro.com/antivirus-evasion-techniques/>

<https://offs3cg33k.medium.com/antivirus-evasion-bypass-techniques-b547cc51c371>

<https://portswigger.net/daily-swig/africa>

<https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-report-identifies-top-cyber-threats-in-Africa> Introduction





Resources

<https://github.com/obfuscar/obfuscar>

<https://github.com/TheWover/donut>

<https://github.com/3xpl01tc0d3r/ProcessInjection>

<https://github.com/jfmaes/LazySign>

<https://rastamouse.me/memory-patching-amsi-bypass/>

<https://gist.github.com/FatRodzianko/e6729fa28d5dfa868520496fc800802d>

<https://pentestlaboratories.com/2021/05/17/amsi-bypass-methods/>



THANKS!



CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik

